

1 **CLAIMS**

2 What is claimed is:

3
4 1. A method comprising:

5 verifying that a first application is authorized to set an initial range for a
6 controlled parameter setting;

7 if authorized, allowing the first application to set an initial range for the
8 controlled parameter setting; and

9 subsequently, allowing at least a second application to modify the
10 controlled parameter setting within the initial range set by the first application.

11
12 2. A method as recited in claim 1, wherein the first application is
13 verified based on a first security code.

14
15 3. A method as recited in claim 2, wherein the first security code is at
16 least partially encrypted.

17
18 4. A method as recited in claim 1, wherein the first application is
19 verified based at least partially on memory location information associated with a
20 verifying function.

21
22 5. A method as recited in claim 4, wherein the memory location
23 information associated with the verifying function defines memory location within
24 a read only memory (ROM).
25

1 6. A method as recited in claim 1, wherein the initial range includes at
2 least a maximum controlled parameter setting, and the second application is not
3 allowed to modify the controlled parameter setting beyond the maximum
4 controlled parameter setting.

5
6 7. A method as recited in claim 1, wherein the initial range includes at
7 least a minimum controlled parameter setting, and the second application is not
8 allowed to modify the controlled parameter setting below the minimum controlled
9 parameter setting.

10
11 8. A method as recited in claim 1, further comprising:
12 verifying that the second application is authorized to modify a current range
13 for the controlled parameter setting;
14 if authorized, allowing the second application to modify the current range
15 for the controlled parameter setting; and
16 subsequently, allowing at least a third application to modify the controlled
17 parameter setting within the current range as modified by the second application.

18
19 9. A method as recited in claim 8, wherein the second application is
20 verified based on a second security code.

21
22 10. A method as recited in claim 9, wherein the second security code is
23 at least partially encrypted.
24
25

1 **11.** A method as recited in claim 8, wherein the second application is
2 verified based at least partially on memory location information associated with a
3 verifying function.

4
5 **12.** A method as recited in claim 11, wherein the memory location
6 information associated with the verifying function defines memory location within
7 a read only memory (ROM).

8
9 **13.** A method as recited in claim 8, wherein the current range includes
10 at least a maximum controlled parameter setting, and the third application is not
11 allowed to modify the controlled parameter setting beyond the maximum
12 controlled parameter setting.

13
14 **14.** A method as recited in claim 8, wherein the current range includes
15 at least a minimum controlled parameter setting, and the third application is not
16 allowed to modify the controlled parameter setting below the minimum controlled
17 parameter setting.

18
19 **15.** A method as recited in claim 1, wherein the controlled parameter
20 setting is selected from a group of settings comprising an audio volume control
21 parameter, an audio tone control parameter, an illumination control parameter, a
22 visual display control parameter, a temperature control parameter, a
23 communication access control parameter, a peripheral device control parameter, a
24 vehicle control parameter, and an environment control parameter.
25

1 16. A method as recited in claim 8, wherein:
2 verifying that the first application is authorized to set the initial range for
3 the controlled parameter setting further includes using a first verifier; and
4 verifying that the second application is authorized to modify the current
5 range for the controlled parameter setting further includes using a second verifier,
6 wherein the first verifier and the second verifier are operatively configured
7 in a serial arrangement, and the first verifier is independently responsive to a first
8 security code and the second verifier is independently responsive to a second
9 security code.

10
11 17. A method as recited in claim 16, wherein the first verifier is
12 provided by a first entity and the second verifier that is provided by a second
13 entity.

14
15 18. A method as recited in claim 16, wherein the first security code and
16 the second security code are the same.

17
18 19. A method as recited in claim 16, wherein the first security code is
19 provided by a first entity and the second security code is provided by a second
20 entity.

1 **20.** A method as recited in claim 1, wherein verifying that the first
2 application is authorized to set the initial range for the controlled parameter setting
3 further includes using at least one verifier selected from a group comprising at
4 least a first verifier and a second verifier.

5
6 **21.** A computer-readable medium as recited in claim 8, wherein
7 verifying that the second application is authorized to set the initial range for the
8 controlled parameter setting further includes using at least one verifier selected
9 from a group comprising at least a first verifier and a second verifier.

10
11 **22.** A computer-readable medium having computer-executable
12 instructions for performing steps comprising:

13 verifying that a first application is authorized to set an initial range for a
14 controlled parameter setting;

15 if authorized, allowing the first application to set an initial range for the
16 controlled parameter setting; and

17 subsequently, allowing at least a second application to modify the
18 controlled parameter setting within the initial range set by the first application.

19
20 **23.** A computer-readable medium as recited in claim 22, wherein the
21 first application is verified based on a first security code.

22
23 **24.** A computer-readable medium as recited in claim 23, wherein the
24 first security code is at least partially encrypted.
25

1 **25.** A computer-readable medium as recited in claim 22, wherein the
2 first application is verified based at least partially on memory location information
3 associated with a verifying function.
4

5 **26.** A computer-readable medium as recited in claim 25, wherein the
6 memory location information associated with the verifying function defines
7 memory location within a read only memory (ROM).
8

9 **27.** A computer-readable medium as recited in claim 22, wherein the
10 initial range includes at least a maximum controlled parameter setting, and the
11 second application is not allowed to modify the controlled parameter setting
12 beyond the maximum controlled parameter setting.
13

14 **28.** A computer-readable medium as recited in claim 22, wherein the
15 initial range includes at least a minimum controlled parameter setting, and the
16 second application is not allowed to modify the controlled parameter setting below
17 the minimum controlled parameter setting.
18

19 **29.** A computer-readable medium as recited in claim 22, having
20 computer-executable instructions for performing steps further comprising:

21 verifying that the second application is authorized to modify a current range
22 for the controlled parameter setting;

23 if authorized, allowing the second application to modify the current range
24 for the controlled parameter setting; and
25

1 subsequently, allowing at least a third application to modify the controlled
2 parameter setting within the current range as modified by the second application.

3
4 **30.** A computer-readable medium as recited in claim 29, wherein the
5 second application is verified based on a second security code.

6
7 **31.** A computer-readable medium as recited in claim 30, wherein the
8 second security code is at least partially encrypted.

9
10 **32.** A computer-readable medium as recited in claim 29, wherein the
11 second application is verified based at least partially on memory location
12 information associated with a verifying function.

13
14 **33.** A computer-readable medium as recited in claim 32, wherein the
15 memory location information associated with the verifying function defines
16 memory location within a read only memory (ROM).

17
18 **34.** A computer-readable medium as recited in claim 29, wherein the
19 current range includes at least a maximum controlled parameter setting, and the
20 third application is not allowed to modify the controlled parameter setting beyond
21 the maximum controlled parameter setting.

1 35. A computer-readable medium as recited in claim 29, wherein the
2 current range includes at least a minimum controlled parameter setting, and the
3 third application is not allowed to modify the controlled parameter setting below
4 the minimum controlled parameter setting.

5
6 36. A computer-readable medium as recited in claim 22, wherein the
7 controlled parameter setting is selected from a group of settings comprising an
8 audio volume control parameter, an audio tone control parameter, an illumination
9 control parameter, a visual display control parameter, a temperature control
10 parameter, a communication access control parameter, a peripheral device control
11 parameter, a vehicle control parameter, and an environment control parameter.

12
13 37. A computer-readable medium as recited in claim 29, wherein:
14 verifying that the first application is authorized to set the initial range for
15 the controlled parameter setting further includes using a first verifier; and
16 verifying that the second application is authorized to modify the current
17 range for the controlled parameter setting further includes using a second verifier,
18 wherein the first verifier and the second verifier are operatively configured
19 in a serial arrangement, and the first verifier is independently responsive to a first
20 security code and the second verifier is independently responsive to a second
21 security code.

22 38. A computer-readable medium as recited in claim 37, wherein the
23 first verifier is provided by a first entity and the second verifier that is provided by
24 a second entity.
25

1 **39.** A computer-readable medium as recited in claim 37, wherein the
2 first security code and the second security code are the same.

3
4 **40.** A computer-readable medium as recited in claim 37, wherein the
5 first security code is provided by a first entity and the second security code is
6 provided by a second entity.

7
8 **41.** A computer-readable medium as recited in claim 22, wherein
9 verifying that the first application is authorized to set the initial range for the
10 controlled parameter setting further includes using at least one verifier selected
11 from a group comprising at least a first verifier and a second verifier.

12
13 **42.** A computer-readable medium as recited in claim 29, wherein
14 verifying that the first application is authorized to set the initial range for the
15 controlled parameter setting further includes using at least one verifier selected
16 from a group comprising at least a first verifier and a second verifier.

17 **43.** A method comprising:
18 setting an authorized range and a current value for a controlled parameter;
19 receiving a request to change the current value of the controlled parameter
20 from an application;
21 changing the current value of the controlled parameter if a requested value
22 of the controlled parameter is within the authorized range;
23 otherwise, verifying that the application is authorized to modify the
24 authorized range for the controlled parameter, prior to changing the current value
25 of the controlled parameter to the requested value.

1
2 **44.** A method as recited in claim 43, wherein verifying that the
3 application is authorized to modify the authorized range for the controlled
4 parameter further comprises changing the authorized range to include the
5 requested value when the application is authorized to modify the authorized range.
6

7 **45.** A method as recited in claim 44, wherein the authorized range
8 includes at least one authorized limit selected from a group including a minimum
9 authorized limit and a maximum authorized limit.
10

11 **46.** A method as recited in claim 45, further comprising changing the
12 current value of the controlled parameter to the minimum authorized limit if the
13 requested value is less than the minimum authorized limit and the application is
14 not authorized to modify the authorized range.
15

16 **47.** A method as recited in claim 45, further comprising changing the
17 current value of the controlled parameter to the maximum authorized limit if the
18 requested value is more than the maximum authorized limit and the application is
19 not authorized to modify the authorized range.
20

21 **48.** A computer-readable medium having computer-executable
22 instructions for performing steps comprising:

23 setting an authorized range and a current value for a controlled parameter;
24 receiving a request to change the current value of the controlled parameter
25 from an application;

1 changing the current value of the controlled parameter if a requested value
2 of the controlled parameter is within the authorized range;

3 otherwise, verifying that the application is authorized to modify the
4 authorized range for the controlled parameter, prior to changing the current value
5 of the controlled parameter to the requested value.
6

7 **49.** A computer-readable medium as recited in claim 48, wherein
8 verifying that the application is authorized to modify the authorized range for the
9 controlled parameter further comprises changing the authorized range to include
10 the requested value when the application is authorized to modify the authorized
11 range.
12

13 **50.** A computer-readable medium as recited in claim 49, wherein the
14 authorized range includes at least one authorized limit selected from a group
15 including a minimum authorized limit and a maximum authorized limit.
16

17 **51.** A computer-readable medium as recited in claim 50, further
18 comprising computer-executable instructions for performing the step of changing
19 the current value of the controlled parameter to the minimum authorized limit if
20 the requested value is less than the minimum authorized limit and the application
21 is not authorized to modify the authorized range.
22
23
24
25

1 **52.** A computer-readable medium as recited in claim 50, further
2 comprising computer-executable instructions for performing the step of changing
3 the current value of the controlled parameter to the maximum authorized limit if
4 the requested value is more than the maximum authorized limit and the application
5 is not authorized to modify the authorized range.

6
7 **53.** A system comprising:
8 at least one processor operatively configured to respond to computer
9 instructions associated with a plurality of applications, including a first
10 application;

11 memory coupled to the processor and configured to store data associated
12 with at least the first application, and

13 a program operatively configured within the processor and memory and
14 arranged to set a parameter value and a range associated with at least one
15 controlled parameter, determine if the first application is authorized to modify the
16 range, modify the parameter value within the range when requested by the first
17 application, and modify the parameter value outside the range and modify the
18 range when requested by the first application if the first application is authorized
19 to modify the range.

20
21 **54.** A system as recited in claim 53, wherein the program determines if
22 the first application is authorized to modify the range by analyzing a security code
23 provided by the first application.
24
25

1 **55.** A system as recited in claim 54, wherein the program decodes the
2 security code and compares the resulting data to predetermined data to determine
3 if the first application is authorized to modify the range.

4
5 **56.** A system as recited in claim 54, wherein the program determines
6 that the first application is authorized to change the range only if the security code
7 matches a valid security code.

8
9 **57.** A system as recited in claim 54, wherein the program further
10 includes at least one linked verifier function stored within a predefined portion of
11 the memory, and the program is configured to determine if the linked verifier
12 function, as called by the program, is not within the predefined portion of the
13 memory, in which case, the program determines that the first application is
14 unauthorized to modify the range.

15
16 **58.** A system as recited in claim 57, wherein the predefined memory
17 location is within a read only portion of the memory.

18
19 **59.** A system as recited in claim 54, wherein the security code is
20 uniquely associated a software developer entity responsible for providing the first
21 application.

1 **60.** A system as recited in claim 53, wherein the processor is operatively
2 configured to respond to computer instructions associated with at least a second
3 application, and the program is further configured to determine if the second
4 application is authorized to modify the range, modify the parameter value within
5 the range when requested by the second application, and modify the parameter
6 value outside the range and modify the range when requested by the first
7 application if the first application is authorized to modify the range.

8
9 **61.** A system as recited in claim 53 wherein the parameter is selected
10 from a group comprising an audio volume control parameter, an audio tone control
11 parameter, an illumination control parameter, a visual display control parameter, a
12 temperature control parameter, a communication access control parameter, a
13 peripheral device control parameter, a vehicle control parameter, and an
14 environment control parameter.

15
16 **62.** A system as recited in claim 53, wherein the processor, the memory,
17 and the program are part of a computer system within a vehicle.

18
19 **63.** A system as recited in claim 53, further comprising at least one
20 device that is coupled to the program and is responsive to the parameter value
21 from the program.
22
23
24
25

1 **64.** An arrangement for use in a computer system, the arrangement
2 comprising:

3 a parameter manager configurable to receive a parameter change request
4 from one or more computer applications and selectively output a corresponding
5 parameter value;

6 at least one verifier function accessible by the parameter manager and
7 configured to determine if the parameter change request is from a computer
8 application that is authorized to exceed a parameter limitation; and

9 a device driver coupled to the parameter manager and configured to receive
10 the parameter value from the parameter manager and output a corresponding
11 control parameter suitable for use by at least one device.

12
13 **65.** An arrangement as recited in claim 64, wherein the verifier
14 determines if the parameter change request is from the computer application
15 authorized to exceed the parameter limitation by analyzing a security code
16 identified by the first application.

17
18 **66.** An arrangement as recited in claim 65, wherein the verifier decodes
19 the security code and compares the resulting data to a valid security code to
20 determine if the computer application is authorized to exceed the parameter
21 limitation.

1 **67.** An arrangement as recited in claim 65, wherein at least a portion of
2 the verifier is invoked by the parameter manager in a predefined, identifiable
3 manner, such that if invoked otherwise the computer application is deemed
4 unauthorized to exceed the parameter limitation.

5
6 **68.** An arrangement as recited in claim 67, further comprising a
7 memory, and wherein the at least a portion of the verifier that is invoked by the
8 parameter manager in a predefined, identifiable manner is associated with at least
9 one memory location within a read only portion of the memory.

10
11 **69.** An arrangement system as recited in claim 64, wherein the security
12 code is uniquely associated a software developer entity responsible for providing
13 the computer application and the verifier.

14
15 **70.** An arrangement as recited in claim 64, wherein the parameter
16 manager, verifier, and device driver are part of a computer system within a
17 vehicle.

18
19 **71.** An arrangement as recited in claim 64, wherein the at least one
20 device includes a computer implemented function.
21
22
23
24
25